Selçuk J. Appl. Math.
Vol. 11. No.2. pp. 71-76, 2010

Selçuk Journal of Applied Mathematics

Cyclic Codes over Some Finite Rings

Mehmet Özen, Murat Güzeltepe

Department of Mathematics, Sakarya University, TR54187 Sakarya, Türkiye
e-mail: mguzeltepe@sakarya.edu.tr

Received Date: Desember 09, 2009
Accepted Date: September 06, 2010

Abstract. In this paper cyclic codes are studied with respect to the Mannheim metric over some finite rings by using Gaussian integers and the decoding procedure for these codes is given.

Key words: Block codes, Mannheim distance, Cyclic codes, Syndrome decoding.
2000 Mathematics Subject Classification. *94B05, 94B60.*

1. Introduction

Mannheim metric, which was initially put forward by Huber in 1994, has been used in many papers so far [1, 2, 3,4, 5]. In 1994, Huber defined the Mannheim metric and the Mannheim weight over Gaussian integers and, eventually, he obtained the linear codes which can correct errors of Mannheim weight one in [1]. Moreover, some of these codes which are suited for quadrature amplitude modulation (QAM)-type modulations were considered by Huber. Later, Huber transferred these codes, which he obtained by using the Mannheim metric and Gaussian integers, into Eisenstein-Jacobi integers in [2]. In 1997, Huber proved the MacWilliams theorem for two-dimensional modulo metric (Mannheim metric) [3]. In 2001, Neto obtained new codes over Euclidean domain $Q\sqrt{d}$, where $d = -1, -2, -3, -7, -11$, in [4] by using the Mannheim metric given in [1, 2]. In 2004, Fan and Gao obtained one-error correcting linear codes by using a novel Mannheim weight over finite algebraic integer rings of cyclotomic fields [5]. In our study, the codes in [1] are transferred into some finite ring by using the Mannheim metric and Gaussian integers. In decoding procedure, some differences occur when these codes are transferred from finite field into finite rings. We also mention these differences.

Section II is organized as follows. In Proposition 1, the necessary algebraic background is revealed in order to obtain cyclic codes. In Theorem 2, it is shown

how to obtain cyclic codes by utilizing Proposition 1, 2 and 3. In Proposition 4, the algebraic background, which is essential for obtaining cyclic code over the other finite rings, is arranged and in Theorem 3, it is shown how to obtain cyclic codes over the other finite rings.

2. Cyclic Codes over Gaussian Integers

A Gaussian integer is a complex number whose real and imaginary parts are both integers. Let G denote the set of all Gaussian integers and let G_π denote residue class of G modulo π, where $\pi = a + ib$ is a Gaussian prime integer and p is a prime integer such that $p = a^2 + b^2 = 4n + 1$ The modulo function $GF(p) \to G_\pi$ is defined by

$$\mu(g) = g - [\frac{g.\pi^*}{p}]\pi, \tag{1}$$

where $GF(p)$ is a finite field with p elements. In (1), the symbol of [.] is rounding to the closest integer. The rounding of Gaussian integer can be done by rounding the real and imaginary parts separately to the closest integer. In view of equation (1), G_π is isomorphic to Z_p, where Z_p is residue class of the set Z of all integers modulo p. Let α and β be elements in G_π then the Mannheim weight of γ is defined by $w_M(\gamma) = |\mathrm{Re}\,(\gamma)| + |\mathrm{Im}(\gamma)|$, where $\gamma = \alpha - \beta \pmod{\pi}$. Since the codes are linear codes, the Mannheim distance between α and β is $d_M(\alpha, \beta) = w_M(\gamma)$ [1].

Theorem 1. If a and b are relatively prime integers, then $G = Z[i]/\langle a + ib\rangle \cong Z_{a^2+b^2}$ [6].

Proposition 1. Let $\pi = a + bi$ be a prime in G and let $p > 2$ be a prime element in Z such that $p = a^2 + b^2 = 4n + 1$. If g is a generator of $G^*_{\pi^2}$, then $g^{\phi(p^2)/4} \equiv i \pmod{\pi^2}$, (or $g^{\phi(p^2)/4} \equiv -i \mod \pi^2$).

Proof. If $|\pi| = 4n+1$ is a prime integer in Z , the real and imaginary parts of π^2 are relatively primes, where the symbol $|\cdot|$ denotes modulo of a complex number. So, G_{π^2} is isomorphic to Z_{p^2} (See Theorem 1). If g is a generator of $G^*_{\pi^2}$, then g, g^2, ..., $g^{\phi(p^2)} \mod \pi^2$ constitute a reduced residue system. Therefore there is a positive integer k as $g^k \equiv i \mod \pi^2$ ($g^k \equiv -i \mod \pi^2$, where $1 \le k \le \phi(p^2)$). Hence, we can infer $g^{4k} \equiv 1 \mod \pi^2$. Since $\phi(p^2) \big| 4k$ and $4 \le 4k \le 4\phi(p^2)$, we obtain $\phi(p^2) = k, \phi(p^2) = 2k$ or $\phi(p^2) = 4k$. If $\phi(p^2) = k$ was equal to k or $2k$, we should have $\pi^2 \big| i - 1$ or $\pi^2 \big| 2$ ($\pi^2 \big| - i - 1$), but this would contradict the fact that $\left|\pi^2\right|^2 > 2$.

Proposition 2. Let $\pi = a + ib$ be a prime in G and let $p > 2$ be a prime in Z such that $p = a^2 + b^2 = 4n + 1$. If g is a generator of $G^*_{\pi^k}$, the $g^{\phi(p^k)/4} \equiv i \pmod{\pi^k}$ or $(g^{\phi(p^k)/4} \equiv -i \pmod{\pi^k})$.

Proof. This is immediate from Proposition 1.

Proposition 3. Let $\pi = a + ib$ be a prime in G and let $p > 2$ be a prime in Z such that $p = a^2+b^2 = 4n+1$. If g is a generator of $G^*_{\pi^k}$ and $g^{\phi(p^2)/4} \equiv i \mod \pi^2$, then $-g$ also becomes a generator of $G^*_{\pi^2}$ such that $(-g)^{\phi(p^2)/4} \equiv -i \mod \pi^2$.

Proof. $g^{\phi(p^2)/4} \equiv i \mod \pi^2$ implies that$(-g)^{\phi(p^2)/4} \equiv -i \mod \pi^2$ since $\phi(p^2) = 4n(4n + 1)$ and n is an odd integer.

Theorem 2. Let $p > 2$ is a prime in Z and $\pi = a + ib$ is a prime in G such that $p = a^2 + b^2 = 4n + 1$ $(a, b, n \in Z)$, then cyclic codes of length $\phi(p^2)/4$ and $\phi(p^2)/2$ are generated over the ring G_{π^2} whose generator polynomials are of the first and second degree, respectively.

Proof. There is an element g of G_{π^2} and $G^*_{\pi^2}$ is generated by g since Z_{p^2} is isomorphic to G_{π^2}. We know that $g^{\phi(p^2)/4} \equiv i \mod \pi^2$ implies that $(-g)^{\phi(p^2)/4} \equiv -i \mod \pi^2$ from Proposition 3. Hence $x^{\phi(p^2)/4} - i$ and $x^{\phi(p^2)/4} + i$ are factored as $(x - g)Q(x) \mod \pi^2$ for $x = g$ and $(x + g)R(x) \mod \pi^2$ for $x = -g$, respectively, where $Q(x)$ and $R(x)$ are the polynomials in the indeterminate X with coefficients in G_{π^2}. Moreover, $x^{\phi(p^2)/2} + 1$ can be factored as $(x-g)(x+g)A(x)$ $\mod \pi^2$, where $A(x)$ is the polynomials in the indeterminate X with coefficients in G_{π^2}.Furthermore all components of any row of generator matrix do not consist of zero divisors since the generator polynomial would be selected as a monic polynomial.

We now explain how to construct cyclic codes over the other finite rings.

Denote Z^*_n by the set of multiplicative inverse elements of Z_n. If $k \geq 1$ and $k| n$ then the set $Z^*_n(k)$ is a subgroup of Z^*_n, where $Z^*_n(k) = \{x \in Z^*_n : x \equiv 1 \mod k\}$. If s and t are relatively prime numbers, then $Z^*_{st}(s) \cong Z^*_t, Z^*_{st}(t) \cong Z^*_s$.

Proposition 4. Let p_1 and p_2 be odd primes and let $\pi_1 = a+bi$ and $\pi_2 = c+di$ be prime Gaussian integers, where $p_1 \neq p_2$ and $p_1 = a^2 + b^2 = 4n_1 + 1$ and $p_2 = c^2 + d^2 = 4n_2 + 1$ $(a, b, c, d, n_1, n_2 \in Z)$. If π_1 and π_2 are Gaussian integers, there exist elements e and f in $G^*_{\pi_1\pi_2}$ satisfying $e^{\phi(p_2)} \equiv 1 \pmod{\pi_1\pi_2}$ and $f^{\phi(p_1)} \equiv 1 \pmod{\pi_1\pi_2}$.

Proof. Let p_1 and p_2 be distinct odd primes. Then p_1 and p_2 are relatively primes. Since s and t are relatively prime numbers, p_1 and p_2 can be chosen as s and t, respectively, that is, $s = a^2 + b^2 = 4n_1 + 1$ and $t = c^2 + d^2 = 4n_2 + 1$. Using (1), we have $Z_s \cong G_{\pi_1}$ and $Z_t \cong G_{\pi_2}$. It is clear that $Z_{st} \cong G_{\pi_1\pi_2}$ from Theorem 1. Thus, we have $G^*_{\pi_1\pi_2}(\pi_1) \cong Z^*_{st}(s) \cong Z^*_t \cong G^*_{\pi_2}G^*_{\pi_2}$ is a cyclic group because π_2 is a prime Gaussian integer. So, $G^*_{\pi_1\pi_2}(\pi_1)$ has a generator. Let's call this generator e. Then $e^{\phi(p_2)} \equiv 1 \pmod{\pi_1\pi_2}$. In a similar way, $G^*_{\pi_1\pi_2}(\pi_2)$

has a generator, let's call it f. Then $f^{\phi(p_1)} \equiv 1 \pmod{\pi_1\pi_2}$ since $G^*_{\pi_1\pi_2}(\pi_2)$ is isomorphic to $G^*_{\pi_1}$.

Proposition 5. Let p_k be distinct odd primes in Z such that $p_k = a_k^2 + b_k^2 = 4n_k + 1$, $\pi_k = a_k + ib_k$ and $a_k, b_k, n_k \in Z$, for $k = 1, 2, ..., m$. Then, there exists an element e_k of $G^*_{\pi_1\pi_2...\pi_m}$ such that $e_k^{\phi(p_k)} \equiv 1 \pmod{\pi_1\pi_2...\pi_m}$.

Proof. This is immediate from Proposition 4.

Theorem 3. Let p_1 and p_2 be distinct od primes in Z and let $\pi_1 = a + bi$ and $\pi_2 = c + di$ be prime Gaussian integers in G, where $p_1 = a^2 + b^2 = 4n_1 + 1$, $p_2 = c^2 + d^2 = 4n_2 + 1$, $n_1, n_2 \in Z$. Then there exists a cyclic code of length $\phi(p_1)$ and $\phi(p_2)$ over the ring $G_{\pi_1.\pi_2}$. The generator polynomial of this cyclic code is a first degree monic polynomial.

Proof. From Proposition 4, $x^{\phi(p_2)} - 1$ can be factored as $(x-e)D(x) \pmod{\pi_1\pi_2}$ since $e^{\phi(p_2)} \equiv 1 \pmod{\pi_1\pi_2}$. If we take the generator polynomial as $g(x) = x - e$, then the generator polynomial $g(x)$ generates the generator matrix. At least one of the components in any row of the generator matrix is not zero divisor.

To illustrate the construction of cyclic codes over some finite rings, we consider examples as follows.

Example 1. The polynomial $x^{10} + 1$ factors over the ring G_{3+4i} as $(x-2).(x-1+i)A(x)$, where $A(x)$ is a polynomial in $G_{3+4i}[X]$. If the generator polynomial $g(x)$ is taken as $x^2 + (1-2i)x + (-2+i)$, then the generator matrix and the parity check matrix are as follows

$$G = \begin{pmatrix} -2+i & 1-2i & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2+i & 1-2i & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2+i & 1-2i & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2+i & 1-2i & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2+i & 1-2i & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2+i & 1-2i & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2+i & 1-2i & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2+i & 1-2i & 1 \end{pmatrix},$$

$$H = \begin{pmatrix} 1 & -(1-2i) & -(-2+i) & -(2+i) & -(1+i) & -(2+i) & 3i & -1+i & 2i & 0 \\ 0 & 1 & -(1-2i) & -(-2+i) & -(2+i) & -(1+i) & -(2+i) & 3i & -1+i & 2i \end{pmatrix},$$

respectively. Let the received vector r be

$$\begin{pmatrix} -2+i & 1-2i & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

First we compute the syndrome S as follows:

$$S = \frac{ix^3 + x^2 + (1-2i)x + (-2+i)}{x^2 + (1-2i)x + (-2+i)} = (1+2i)x + (2+i).$$

Therefore, from Table I, it is seen that the syndrome $S \equiv ix^3$. Notice that first we compute the syndrome of the received vector to be decoded. If this syndrome does not appears in Table I, then its associates should be checked. Thus, the

received vector r is decoded as $c(x) = r(x) - ix^3 = x^2 + (1-2i)x + (-2+i)$. Finally we get
$c = \begin{pmatrix} -2+i & 1-2i & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

Example 2. Let $p_1 = 5$, $p_2 = 13$. Let the generator polynomial $g(x)$ and the parity check polynomial $h(x)$ be $x-3-i$ and $x^3+(3+i)x^2+(4-i)x+2-2i$, respectively. Then we obtain the generator matrix G and parity check matrix H as follows, respectively;

$$G = \begin{pmatrix} -3-i & 1 & 0 & 0 \\ 0 & -3-i & 1 & 0 \\ 0 & 0 & -3-i & 1 \end{pmatrix},$$

$$H = \begin{pmatrix} 1 & 3+i & 4-i & 2-2i \end{pmatrix}.$$

Assume that received vector is $r = \begin{pmatrix} -3-i & 1 & i & 0 \end{pmatrix}$. We compute the syndrome as

$$\frac{r(x)}{g(x)} = \frac{ix^2+x-3-i}{x-3-i} = (x-3-i)(ix+3i) + (1+4i).$$

Since $1+4i \equiv x^2.i$, the vector $r(x)$ is decoded as $c(x) = r(x) - ix^2 = x-3-i$. In Table II, coset leaders and their syndromes are given.

3. Conclusion

In this paper we obtained cyclic codes over some finite Gaussian integer rings and we gave decoding procedure for these codes.

0	0	x^6	$(-2-i)x+3i$
1	1	x^7	$3ix+(2+i)$
x	x	x^8	$(-1+2i)x+2i$
x^2	$(-1+2i)x+(2-i)$	x^9	$2ix+(1-2i)$
x^3	$(2-i)x+(1-2i)$	x^10	-1
x^4	$(-2-i)x+(-1-i)$	x^11	$x^{11} = x^{10}x$
x^5	$(-1-i)x+(2+i)$	x^12	$x^{12} = x^{10}x^2$

Table 1. The coset leaders and their syndromes.

0	0
1	1 (and its associates)
x	$3+i$ (and its associates)
x^2	$4-i$ (and its associates)
x^3	$2-2i$ (and its associates)

Table 2. The coset leaders and their syndromes.

References

1. Huber K., "Codes Over Gaussian Integers" IEEE Trans. Inform.Theory, vol. 40, pp. 207-216, jan. 1994.
2. Huber K., "Codes Over Eisenstein-Jacobi Integers," AMS, Contemp. Math., vol. 158, pp. 165-179, 1994.
3. Huber K., "The MacWilliams theorem for two-dimensional modulo metrics" AAECC Springer Verlag, vol. 8, pp. 41-48, 1997.
4. Neto T.P. da N., "Lattice Constellations and Codes From Quadratic Number Fields" IEEE Trans. Inform. Theory, vol. 47, pp. 1514-1527, May 2001.
5. Fan Y. and Gao Y., "Codes Over Algebraic Integer Rings of Cyclotomic Fields" IEEE Trans. Inform. Theory, vol. 50, No. 1 jan. 2004.
6. Dresden G. and Dymacek W.M., "Finding Factors of Factor Rings Over The Gaussian Integers" The Mathematical Association of America, Monthly Aug-Sep. 2005.